Joint Engineering Team (JET) Meeting Minutes

National Coordination Office for Networking and Information Technology R&D (NCO/NITRD)
490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024
July 21, 2020 12:00-2:00 p.m. ET

Participants

Donald Anderson, NASA
Shawn Armstrong, University of Alaska
Jeff Bartig, Internet2
Joe Breen, UTEN/University of Utah
Aaron Brown, SNL
Nick Buraglio, ESnet
Scott Campbell, ESnet
Rich Carlson, DOE/SC
Brian Cashman, Internet2
Sean Connelly, DHS
Shaw Cronin, NASA
Basil Decina, NRL
Dave Diller, MAX
Eric Estes, NOAA
Bill Fink, NASA/GSFC
Dale Finkelson, Internet2
Andrew Gallo, CAAREN/GWU
Paul Howell, Internet2
Ann Keane, NOAA
Jonah Keough, PNWGP/Pacific Wave
Kevin Kranacs, NASA/GSFC – EOS
Michael Lambert, PSC/3ROX
Craig Lee, The Aerospace Corporation
Paul Love, NCO/NITRD
Howard Lu, NIH
Bryan Lyles, ORNL
Joe Mambretti, StarLight/MREN
Dave Mauro, NOAA
Linden Mercer, NRL
Christopher Mishaga, NASA/GSFC
Jenny Moniz, DHS
Alex Moura, RNP
Aruna Muppalla, NASA/GSFC
Anne Richeson, CenturyLink
Frank Seesink, University of North Carolina
Dan Taylor, Internet2
Kevin Thompson, NSF
Catherine Traini, DHS
George Uhl, NASA/GSFC
Matt Zekauskas, Internet2

Proceeding: This meeting was chaired by Kevin Thompson (NSF) and Rich Carlson (DOE/SC).

I. **Action Items**:

- Discuss potential JET tasking for CY20 at August meeting
- Discussion of the current draft of OMB's memo on the transition to IPv6
  note: Set for initial discussion at August meeting.
- ESnet update on its operational network security use of Rapid7.
- Internet2 and ESnet updates on their respective new networks.

II. **Review of the Minutes** of the June meeting: Corrections were received after the meeting. The Meetings of Interest section was updated to reflect changes due to COVID-19.

III. **Overview of TIC 3.0 – Sean Connelly (DHS – Cybersecurity and Infrastructure Security Agency)**

The slides for this presentation can be found on the JET's web page: Overview of TIC 3.0

A. OMB issued a draft memo in September 2019 modernizing the TIC guidance. It reflects the way networks have evolved in the last decade with remote network use, cloud services, SDNs, and mobile devices . For TIC 1 and TIC 2 the model assumed on premise users with all federal traffic routed through less than 50 access points. The network was the boundary for protection. For TIC 3 there are new flexible alternative security architectures that make use of telemetry to foster situational awareness to both the agencies and CISA. It gives broader authority to the individual agencies. The shift from a single network boundary to distributed, secure architectures is the most significant, fundamental change in TIC. This permits the transition to a security boundary comprised of multiple trust zones. Traffic with the internet is no longer constrained to transit one existing TICAPs.

B. DHS released a set draft documents for the core of TIC 3.0 program guidance in December 2019. Related documents were published by NIST on Zero Trust Architecture, GSA in the Enterprise Infrastructure Solutions Acquisition Vehicle (EIS), and DHS/CISA related to cloud telemetry and monitoring.

C. Evolving Networks and Evolving Security Challenges
    a. As network usage has become more distributed attacks are moving from services and devices on an agency premises to targeting mobile users.
    b. With the surge in telework this spring there is increasing demand to access cloud services directly, bypassing agency physical locations.
    c. Remote users and their use of distributed, perhaps cloud based, services require decentralized security capabilities.
    d. Access decisions, though centrally managed, can be enforced at the endpoint, rather than an agencies premises, and need to be based on the entity's identity and contextual information. Access (trust) can be continuously evaluated during the session. This is assisted by the emergence of better risk detection tools from security and cloud providers. These tools have better detection accuracy and growing automation.
    e. In TIC 2 the Trust Zone might be an agency's entire network. In TIC 3 it can be the same, but it may be as small as a user's mobile device. This fine granularity allows an entity to be authorized to use many different services, again fine grained, and only as needed. The definition of Trust Zones is left to agencies – as fine or coarse grained as fits their needs.
    f. Zero Trust, where all uses and access requests are assumed to be suspect, is a key piece to fine grained Trust Zones. Trust has a half-life, it expires, and must be monitored, reassessed and reestablished. This applies to both the user and a system. The pieces for this are:
        i. Robust Identity, Credential, and Access Management (ICAM)
        ii. Access Controls
        iii. Network Analysis

v. Telemetry
vi. Threat Intelligence

D. Due to COVID OMB released a memo in March 2020 titled "Harness Technology to Support Mission Continuity". The TIC program then released "TIC 3.0 Interim Telework Guidance" (ITG) in April 2020.
   a. It was aimed at the surge in remote use.
   b. It is discretionary for agencies, is interim and not part of the core TIC 3.0 program.
   c. It is valid for only CY2020. Lessons Learned from this temporary solution will be used in the formulation of the "Remote User Use Case" which will be part of the core TIC 3.0 guidance and is expected to be released by the end of 2020.

E. The ITG accommodates the traditional (aka Castle), micro-segmented (City) and Zero Trust (No) security perimeters.
   a. Designed to support a wide variety of connectivity models and to be adapted by agencies for practical teleworking implementations.
   b. Traffic with the public internet must still pass through a TICAP and its EINSTEIN sensors.
   c. Agencies wishing to make use of the ITG must work with service providers. The service providers will map their offerings to the TIC telework capabilities. Agencies can then choose from these offerings.
      i. Agencies are responsible for the selection and understanding what is provided and what gaps may exist.
      ii. Service providers are responsible for taking the CISA supplied template and mapping that to what they provide. These are expected to vary between providers.
      iii. CISA will not endorse any offerings, validate the implementations nor adjudicate any issues.
      iv. In response to a question it isn't yet resolved how/where agencies can look for reported issues with vendor offerings not being as claimed.

F. The National Cybersecurity Protect System (NCPS) in DHS is working to ensure security monitoring, capture and analysis for cloud-based data, services and traffic. They have released a draft of the first volume of the Cloud Interface Reference Architecture.

G. GSA and CISA are working with EIS vendors to offer, in addition to the current MTIPS, TIC services that use cloud-based tools – the Managed Security Services.

H. Everything (interim guidance, security architecture, NIST documents, etc.) all feed into the agencies' risk management planning. TIC 3 is designed to be flexible, to let each agency fit it to their requirements. CISA, OMB & GSA will release additional use cases as technology changes, attach patterns migrate, etc.

I. Resources:
   a. Final TIC 3.0 documents will be released summer 2020 (Remote User Case is targeted for December):
      www.cisa.gov/trusted-internet-connections
   b. CISA TIC website, including an FAQ:
      https://www.cisa.gov/trusted-internet-connections

c. TIC webinar recording on GSA YouTube:
https://www.youtube.com/watch?v=SWkiR3HAEf8

IV. D**iscussion of the JET's tasking on tools to help with inter-domain issues - Joe Breen, all**

A. Background on efforts lead by Eric Boyd, Joe Breen, James Deaton, Dan Doyle, Dale Finkelson and Karl Newell:
   a. The project gets basic SNMP metrics from groups around the country that are willing to share for trouble shooting and research. Metrics include link utilization, discards and errors. These are collected hop by hop as the path crosses multiple domains.
   b. Several prototypes are going along with the drafting of a basic letter of intent for those wishing to participate.
   c. Tools: Telegraf container as an option for local collection. Nearly ready for production use.
   d. Tracking sheet of networks willing to share data. Please update your network's entry. See:
   https://docs.google.com/spreadsheets/d/1pMW_PNVpeT42nAxa3bW4QostMxccHTXkWSPbZOplFwE/edit#gid=0
   The spreadsheet also has an embedded link to measurement templates for campus, regional and national networks setting out what data is desired. See:
   https://drive.google.com/drive/folders/1l-LRyril6u4AvBeY6NlvyYYalNRpjByA
   e. The Internet2 Performance Working Group Community Measurement, Metrics, and Telemetry project holds meetings on the second Tuesday for those participating or interested. If you are interested, please contact Joe:
   Joe Breen <Joe.Breen@utah.edu>

B. Prototype/pilot status:
   a. University of Michigan and Link Oregon: Both continue and need follow-ups.
   b. University of Utah and UETN: Expanding their effort. UETN has hired a full-time person with the object being that all its routers will use telemetry. The university is moving from having telemetry from just the few of its science DMZs that was done for the original demonstration to having telemetry from all.
   c. GÉANT, JISC and Imperial College of London: This is ramping up with initial tests underway between the DTN end points. Compared to earlier pilots, this pilot has a much longer, more complex path to follow and visualize.
   d. University of Hawaii: Discussions are continuing. It is willing to test using the new container.
   e. Clemson University remains interested in doing a pilot.
   f. A new visualization tool for displaying the augmented traceroute is under development. A demonstration in the next month or two.
   g. Work is underway to get the pilots and their status up on the project's wiki.

C. Letter of Intent to Share: *n.b.: The text of the rough draft letter is appended in the appendix to these minutes. See page 8.*

D. The rough draft of the Letter of Intent to Share is the result of extended discussions by those on the project team, with comments from members of The Quilt, DREN and N-

Wave. The goal remains for those who govern the institutions involved to be given a clear understanding of what is being shared, how it's being shared and with whom. After discussion there no further changes suggested by those on the call. (Nor had any been received by email.)
The rough draft will be reviewed at the project team's next meeting.
Kevin Kranacs and George Uhl (both EOS – NASA/GSFC) noted that EOS was precluded by NASA from sharing this data. EOS has an internal perfSONAR (pS) mesh. They are happy to open their firewalls to permit pS testing by prior arrangement. Contact George at:

"Uhl, George D." <george.d.uhl@nasa.gov>

V. O**perational network security roundtable** (only networks with comments are noted)

A. Internet2 (Paul Howell):
    a. Internet2 (I2) enabled Flowspec in the network earlier this year. Currently only available internally to I2 engineers to mitigate against attacks crossing the network. In the future I2 hopes to be able to expose this to others in the R&E community as part of its Next Generation network.
    b. I2 is planning to do a security risk assessment of its cloud connect offering. The offering provides members a mechanism to obtain essentially a private connection to one of the three major cloud providers. Targeted for late summer or early fall.
B. ESnet (Nick Buraglio):
    a. Also looking at Flowspec. Looking at ways ESnet can expose that to the labs giving the labs local control and enabling ESnet to focus on other areas. Anticipated to be deployed as part of ESnet6.
    b. ESnet has had discussions with a couple of companies working on IPv6 security tools.

VI. **Networks Round Table**

A. CAAREN (Andrew Gallo): No update.
B. ESnet (Nick Buraglio):
    a. ESnet6:
        i. The expansion of the OLS continues.
        ii. The packet RFP award is due shortly.
    b. Nick was invited to do a webinar on Segment Routing with Jeff Tantsura.
    c. ESnet is migrating their routing to label based next hop.
C. NASA EOS (Kevin Kranacs): No changes.
D. NASA GSFC (Bill Fink): Working with NRL and StarLight to investigate network topologies for possibly virtual demonstrations in the event SC20 goes virtual. These will use bandwidth between Washington, D.C., and Chicago, IL.
E. NOAA/N-Wave (Ann Keane): No changes.
F. NRL (Linden Mercer): No changes.
G. Pacific Wave (Jonah Keough):

a. Pacific Wave's core switch upgrades (to Juniper MK10s) are proceeding on plan. There have been a couple of minor delays primarily due to scheduling. The Los Angeles, CA, and Seattle, WA, switches are well along. The upgrade is expected to be completed in the fall.
b. Pacific Wave (PW) is investigating some MPLS-VPN options to deploy across the backbone.
c. In fall PW is considering deploying a new circuit between Denver, CO, and Los Angeles that would bypass Albuquerque, NM, and El Paso, TX.

H. RNP (Alex Moura):
a. RNP has installed 100G waves between Fortaleza and Salvador. It is still in the process of installing the fiber and optical hardware to the northeast with other regions.
b. It is still working to extend its optical network from the RNP PoP in Fortaleza to the cable station to connect with the South Atlantic Cable System cable to Angola and then onward to South Africa.
c. With recent upgrades there's now 600Gs between Miami, FL, and Brazil spread between São Paulo and Fortaleza.
d. It has a research and development project underway to build an automated mechanism to collect data sets from measurement and monitoring tools. These would be provided to the research community.

I. 3ROX (Michael Lambert): No network updates from 3ROX, PSC or XSEDE.
J. University of Alaska (Shawn Armstrong): The new terrestrial path, AlCan ONE, has been completed by Matanuska Telephone Association (MTA). It is designed to carry MTA's traffic to the lower 48 thereby mitigating the payments to other carriers for transport. Currently it doesn't offer capacity to other Alaskan carriers. The university is continuing discussions with MTA in hopes being able to use this new path.

VII. **Exchange Points Round Table**

A. PNWGP (Jonah Keough): No updates.
B. WIX and MAN LAN (Dale Finkelson via email): No updates.
C. MAX (Dave Diller): MAX is working on a data center optimization project to support the University of Maryland's moving much of its data into the cloud. MAX also runs the university's HPC which is set for a refresh post-COVID - another influence on the data center's location. The same space will host a new research .
D. StarLight (Joe Mambretti): With SC20 now virtual StarLight (SL) is preparing a set of virtual, large scale demonstrations with GSFC and NRL as Bill Fink mentioned. SL is also working with SCinet on some type of event, perhaps a virtual workshop, to showcase the demonstrations. SL is also involved in some new testbeds. More details on those next month.

VIII. **Other items - Rich Carlson:**

A. Small Business Innovator Research/Technical Transfer (BIR/STTR) has released a new batch of Topics on July 13, 2020, for awards. Two types of tools are included: 1) To

anonymize data so that it can be made available to the research community and 2) To correlate higher level trace data with log data.

a. There will be a network research topic in in the Phase I Release 1 Topic Document of the portfolio. There will be a webinar on July 20, 2020, were the Topics will be described and questions answered. General information is available off the following link:
   https://science.osti.gov/sbir/Funding-Opportunities/FY-2021
b. Details of this Topics can be found at:
   https://science.osti.gov/-/media/sbir/pdf/TechnicalTopics/FY2021_Phase_I_Release_1_Topics.pdf?la=en&hash=D7C553C3316BF15F3A73AEA0CAED21A161692F2B
   If you have ideas on how to improve the use the network data collected take a look when this comes out. While a lab or academic institution can't be the prime it can certainly be a subcontractor. If you're interested form a partnership with a commercial company and submit a proposal.

B. The JET needs to send to the LSN a list of possible taskings to the JET by the end of September.

Meetings of Interest 2020

Note: Meetings cancelled since the July JET have been removed from this list. Those moved to a virtual format have been updated.

Jul 25-31	IETF 108, in person cancelled, moved to a virtual meeting
Jul 27-31	PEARC20, virtual meeting
Aug 3-7	APAN50, in person cancelled, moved to a virtual meeting
Sep 14, 2-4PM UTC *or* Sep 15, 7-9AM UTC	GNA Technical WG, in person cancelled, moved to a virtual meeting
Sep 15-17	NORDUnet 2020, Reykjavik, Iceland *Postponed to Sep 14-16, 2021*
Sep 16-17	LHCOPN/LHCONE meeting #45, virtual meeting
Sep 30 – Oct 1	The Quilt Fall Member Meeting, virtual meeting
Oct 6-7	TechEXtra, virtual meeting
Oct 19-21	NANOG 80, in person cancelled, moved to a virtual meeting
Oct 14-15 & 23	ARIN 46, in person cancelled, moved to a virtual meeting
Nov 14-20	IETF 109, Bangkok, Thailand
Nov 15-20	SC20, in person cancelled, moved to a virtual meeting

Next JET meetings

Note: It is anticipated that JET meetings through the end of CY2020 will be virtual due to COVID-19 guidelines, the JET's usual summer schedule and SC20 moving to a virtual format.

Aug 18	12-2 p.m. ET
Sep 15	12-2 p.m. ET
Oct 20	12-2 p.m. ET
Nov 17	12-2 p.m. ET

Appendix: Rough Draft Letter of Intent to Share

Letter of Intent to Share

Community Measurement, Metrics and Telemetry

ROUGH DRAFT

The focus of this document is to answer: Are we willing to share our respective basic data? What are we agreeing to gather? With whom are we sharing the data?

The organization _____ agrees to collaborate with the Research and Education community to provide its data in a community effort to expose basic metrics, as described in Appendix A, from "End point of interest" to "End point of interest"[1] across the regional, national and international research and education networks. The metrics explicitly do not include regulated data[2]. The organization _____, (hereafter noted as the **Data Owner**) owns the data it provides and is willing to share these basic metrics for the use of enabling better operational visibility for the research and education community and to provide better data for large scale research. These data will help in troubleshooting end to end performance issues, provide baseline information for network tools, and serve for academic research use.

For purposes of this letter the "research and education community" is defined as Internet2, its international peer networks, Internet2's member institutions & RONs, the members of Internet2's peer networks, and US federal research and engineering networks.

The Data Owner agrees to provide its basic metrics via its own exposed API or by collaborating with a known collector entity (see list below for examples) using SNMP or streaming telemetry. The Data Owner will determine the scope of infrastructure metrics which it will expose. This scope must meet the Data Owner's security constraints while simultaneously sharing as much of the basic metrics as feasible to the community. The Data Owner has the right to withdraw its data at anytime from sharing.

The Data Owner may expose its data through several methodologies, such as:

- Provide direct SNMP query capabilities to a known collector entity,

[1] Examples include Science DMZ to Science DMZ, Data Transfer node to Science instrument, network border to Data Transfer node, etc.

[2] Examples include various PII such as HIPAA, PHI, PCI, and other sensitive or confidential data such as regulated by GDPR or similar

- Provide aggregate SNMP information through a community container to a known collector entity[3]
- Provide streaming telemetry aggregate metrics through a community container to a known collector entity
- Provide a local repository which is queryable through a mechanism such as an API[4]
- Other to be determined

These data will be available to query and visualize by community tools and other members in the community. For example, the Augmented Traceroute Report is able to leverage these data to provide end to end lookups of hops along the path where data are being collected regardless of which network(s) it crosses.

All data collected will be queryable within the Research and Education community. In cases where a known collector entity is directly collecting data from a partner network's devices, the known collector entity must securely store all credential information used to collect data with the proper security controls. All participants agree to treat the Data Owner's data with requisite security and privacy controls. All participants agree to use these data towards the mutual benefit of community research and operations.

[3] Examples might include a a large scale science project, a regional network, the Indiana University Global Research NOC, or some other third party collection entity
[4] Examples include ESnet Netbeam API, Measurement Lab datasets, RIPE NCC API

[Letter of Intent to Share] Appendix A:

This appendix represents the technical details of what network

Campus_template - https://docs.google.com/spreadsheets/d/1v7iFw8_YoMpa3wjgwcmlZgy0QsTi1bHb4Qk1cV6qfAM/edit#gid=1161461998

Regional_Template https://docs.google.com/spreadsheets/d/1ElqYjLTLn-Q07doDzHb5vtUCUosFLNbNSgiumm145d4/edit?usp=sharing

National_Backbone_Template https://docs.google.com/spreadsheets/d/14CQi67LjJ_hlnrpjL8WpTbHmQSW112zzvKPBp6fx8Gw/edit?usp=sharing

Some example SNMP variables: (need to put in a template)

set snmp view internet2-view oid 1.3.6.1.2.1.1 include # system (eg. sysUpTime)
| set snmp view internet2-view oid 1.3.6.1.2.1.2 include # IF-MIB

1.3.6.1.2.1.31.1.1.1.6 # ifHCInOctets
1.3.6.1.2.1.31.1.1.1.10 # ifHCOutOctets
1.3.6.1.2.1.31.1.1.1.1 # ifName
1.3.6.1.2.1.31.1.1.1.18 # ifAlias
1.3.6.1.2.1.2.2.1.14 # ifInErrors
1.3.6.1.2.1.2.2.1.20 # ifOuterrors
1.3.6.1.2.1.2.2.1.11 # ifInUcastPkts
1.3.6.1.2.1.2.2.1.17 # ifOutUcastPkts
1.3.6.1.2.1.2.2.1.13 # ifInDiscards
1.3.6.1.2.1.2.2.1.19 # ifOutDiscards
1.3.6.1.2.1.2.2.1.7 # ifAdminStatus
1.3.6.1.2.1.2.2.1.8 # ifOperStatus
1.3.6.1.2.1.4.20.1.2 # ipAdEntIfIndex (yields IP address for pulling up in Traceroute visualization)